

What is Claimed is:

- 425
A4
1. A method of maintaining images in a database, wherein a first image includes a digital watermark embedded therein, the digital watermark comprising a first unique identifier, said method comprising the steps of:
- storing the first image to be indexed by the first unique identifier;
 - storing information related to the first image; and
 - linking the first image and the related information by the first unique identifier.
2. A method according to claim 1, further comprising the steps of:
- in the database, storing at least a second image and linking the first image and the second image with the first unique identifier.
3. A method according to claim 2, wherein the second image comprises a derivative of the first image.
4. A method according to claim 3, wherein the second image includes a digital watermark embedded therein, the digital watermark comprising a second unique identifier, and wherein said method further comprises the step of linking the second unique identifier to the first unique identifier.
5. A method according to claim 3, wherein the related information comprises a history of the image.
6. The method according to claim 5, wherein the history comprises at least one of user usage, creation time, transmission, printing, and image checkout.
7. The method according to claim 1, wherein the database comprises a plurality of databases.

T095150:922500

8. The method according to claim 1, wherein the related information comprises at least one of metadata, location, date, permission level, security access levels, analyst comments, notes, files, and past usage information.

9. A method for managing images, the images including a first image comprising a first identifier steganographically embedded in the first image in the form of a digital watermark, said method comprising the steps of:

retrieving the first image from a database;
altering the first image to create a second image;
steganographically embedding a second identifier in the second image in the form of a digital watermark; and
associating the second image in the database with the first identifier.

10. The method according to claim 9, further comprising the step of removing the first identifier from the second image.

11. The method according to claim 9, further comprising the step of altering the first identifier in the second image.

12. The method according to claim 9, further comprising the step of storing information related to the first image in the database.

13. The method according to claim 12, wherein the related information comprises at least one of metadata, location, date, permission level, security access levels, analyst comments, notes, files, and past usage information.

14. The method according to claim 13, wherein the database comprises a plurality of databases.

TOP SECRET

15. A method to monitor images in a system, the system comprising at least a first user terminal to communicate with a second user terminal and with a database, the images comprising at least a first image digitally watermarked to include a first identifier, said method comprising the steps of:

determining a security level associated with the first image;
comparing the first image security level with a user security level; and
allowing access to the first image based on a result of said comparison step.

16. The method according to claim 15, further comprising the step of recording a transmission in the database of the first image from the first user terminal to the second user terminal.

17. The method according to claim 15, wherein said determining step comprises the steps of:

decoding the digital watermark to determine the first identifier; and
interrogating the database with the first identifier to retrieve the security level.

18. The method according to claim 15, wherein said first image's digital watermark includes security level data, and wherein said determining step comprises the step of decoding the digital watermark to determine the security level.

19. The method according to claim 15, wherein the user security level comprises at least one of a security level for a user and a security level for a user terminal.

20. The method according to claim 19, wherein when the result is a match between the first image security level and the user security level access is allowed.

21. The method according to claim 20, wherein the match indicates that the user security level is equal to or greater than the first image security level.

2025-05-15 09:55:00

22. The method according to claim 15, further comprising the step of recording access to the image.

23. A system comprising:

a first user terminal;

a second user terminal;

a database, wherein the first user terminal and the second user terminal are in communication, and the first user terminal and the second user terminal are each in communication with the database; and

a gatekeeper to regulate the flow of an least a first image between the first user terminal and the second user terminal, wherein the first image comprises at least a first digital watermark including a first identifier, said gatekeeper to determine a security level associated with the first image, compare the first image security level with a user security level, and to allow access by the second user terminal to the first image based on a result of the comparison.

24. A system according to claim 23, wherein said gatekeeper records in the database a transmission of the first image from the first user terminal to the second user terminal.

25. A system according to claim 23, wherein said gatekeeper comprises software to decode the digital watermark to determine the first identifier, and to interrogate the database with the first identifier to retrieve the security level.

26. A system according to claim 23, wherein said first image digital watermark includes security level data, and wherein said gatekeeper comprises software code to decode the digital watermark to determine the security level data.

27. A system according to claim 23, wherein the user security level comprises at least one of a security level for a user and a security level for a user terminal.

28. A module for use in a network comprising at least a first terminal in communication with a database, said module to monitor the flow of an least a first image at a first network location, the first image comprising at least a first digital watermark including a first identifier, said module comprising:

means for determining a security level associated with the first image;
means for comparing a first image security level with a user security level; and
means for allowing access to the first image based on a result of said comparing means.

29. The module according to claim 28, wherein the first image comprises a second digital watermark, the second digital watermark comprising a fragile watermark.

105150-054504